UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/811,551	03/20/2001	Takeshi Shimoyama	1341.1090	9098

21171 7590 09/09/2004

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
NORRIS, TREMAYNE M	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/811,551	SHIMOYAMA ET AL.	
	Examiner	Art Unit	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-12,14-22* is/are rejected.

7)☒ Claim(s) *3 and 13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/21/03; 3/20/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 4 and 14 are objected to because of the following informalities: On page 15 of the specification it states that the addition unit adds a constant to an "even" number-th element, and that the multiplication unit multiplies an "odd" number-th element. However, in claims 4 and 14, it states that the addition unit adds a constant to an "odd" number-th element, and that the multiplication unit multiplies an "even" number-th element. Appropriate correction is required.

2. Claims 9 and 19 are objected to because of the following informalities: The phrase "elementXleftwardsby1bit" in claims 9 and 19 needs spacing between words.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1,2,11,12,21,22 are rejected under 35 U.S.C. 102(a) as being anticipated by Kanda et al (EP 1001398).

Regarding claim 1, Kanda teaches an extended key preparing apparatus wherein extended keys are prepared in common key cryptosystem from cryptographic key input, comprising:

a dividing unit which divides binary digit string of said cryptographic key into a plurality of elements each composed of a predetermined bit length;

an intermediate data preparing unit which prepares plurality of intermediate data by applying a plurality of times an operation wherein a predetermined constant is used to the respective elements divided by said dividing unit;

a selecting unit which selects a plurality of intermediate data corresponding number stages of extended keys from the plurality of the intermediate data prepared by said intermediate data preparing unit; and

an extended key preparing unit which prepares the extended keys corresponding said number of stages by converting irreversibly the plurality of the intermediate data selected by said selecting unit (page 1 lines 5-7; page 1 lines 43-45; page 4 lines 49-56; page 5 lines 41-48; fig.3; fig.4).

Regarding claim 2, Kanda teaches intermediate data preparing unit is provided with a nonlinear type operating unit for effecting nonlinear type operation with respect to the respective elements divided by said dividing unit (fig.4; page 4 lines 49-56; page 5 lines 41-45).

Claims 11, 21,22 are substantially equivalent to claim 1, therefore claims 11,21,22 are rejected because of similar rationale.

Claims 12 is substantially equivalent to claim 2, therefore claims 12 is rejected because of similar rationale.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4-7, 14-17 rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda, and further in view of Vanstone et al.

Regarding claim 4 Kanda teaches the apparatus according to claim 2. What Vanstone teaches that Kanda does not teach is an extended key preparing apparatus according to claim 2 wherein said intermediate data preparing unit is provided with:

an addition unit which adds a constant to an odd number-th element that has been subjected to nonlinear type operation;

a multiplication unit which multiplies an even nurnber-th element which has been subjected to nonlinear type operation by said constant; and

an exclusive OR operating unit which effects exclusive OR operation of said odd number-th element to which has been added the constant and said even number-th element which is succeeding to said odd number-th and to which has been multiplied by said constant (fig.7.11; pages 263-266). It would have been obvious to one of ordinary skill in the art to have combined Kanda's ciphering apparatus with Vanstone's teaching of block ciphering in order to better facilitate the desired security features of confidentiality, authentication, and integrity needed for secure communications (Vanstone page 223-224).

Regarding claim 5, Kanda and Vanstone in combination teach the apparatus according to claim 4, in addition Vanstone teaches a unit for preparing intermediate data by subjecting nonlinear type operation to the result of said exclusive OR operation of said odd number-th element and said even number-th element which is succeeding to said odd number-th (pages 263-266).

Regarding claim 6, Kanda and Vanstone in combination teach the apparatus according to claim 4, in addition Vanstone teaches said addition unit and said multiplication unit repeat the plurality of times additions and multiplications by the use of the number i of different constants, respectively, to prepare the number i of data in every elements; said exclusive OR operating unit repeat i times operations for acquiring

exclusive OR of the odd number-th element and the even number-th element which have been operated by the use of the same constants; and said preparing unit prepare the number i of intermediate data in every elements (pages 263-266).

Regarding claim 7, Kanda and Vanstone in combination teach the apparatus according to claim 4, in addition Kanda teaches selecting unit selects one intermediate data corresponding to said number of stages of an extended key among the number i of intermediate data contained respective elements which have been prepared by said intermediate data preparing unit (fig.4; page 6 paragraph 29).

Claims 14-17 are substantially equivalent to claims 4-7 respectively, therefore claims 14-17 are rejected because of similar rationale.

7. Claims 8,9,18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda, and in further view of Ohmori et al (US pat 6,570,989).

Regarding claim 8, Kanda teaches the apparatus according to claim 1. What Ohmori teaches that Kanda does not teach is a rearrangement unit which rearranges a plurality of intermediate data selected by said selecting unit (co.12 lines 35-47); and an irreversible conversion unit which converts irreversibly the plurality of intermediate data that have been rearranged by said rearrangement unit (col.13 line 8 thru col.14 line 48). It would have been obvious to one of ordinary skill in the art at the time of the invention

to combine Kanda's ciphering apparatus with Ohmori's cryptographic processing apparatus in order to realize high-speed cryptographic processing without the loss of security (Ohmori col.7 lines 25-35).

Regarding claim 9, Kanda and Ohmori in combination teach the method according to claim 8, in addition Ohmori teaches an extended key preparing apparatus according to claim 8 wherein when intermediate data are rearranged in an order of elements X, Z, Y, and W by said rearrangement unit, said irreversible converting unit prepares a first data by adding the element Y to a data obtained by shifting the element X leftwards by I bit; prepares a second data determined by sifting cyclically the data leftwards by further 1 bit, which data has been obtained by subtracting element W from obtained shifting cyclically said element Z leftwards by 1 bit; and operates exclusive OR of said first data and said second data (col.13 line 10 thru col.14 line 48).

Claim 18 is substantially equivalent to claim 8, therefore claim 18 is rejected because of similar rationale.

Claim 19 is substantially equivalent to claim 9, therefore claim 19 is rejected because of similar rationale.

8. Claims 10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda.

Regarding claims 10 and 20, examiner takes official notice that cryptographic keys of different lengths, such as 128 bits, 192 bits, and 256 bits, are well known in the cryptography art. It would have been obvious to one of ordinary skill in the art to use any desired length of key in order to provide the desired level of security.

Allowable Subject Matter

9. Claims 3 and 13 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. The following is a statement of reasons for the indication of allowable subject matter:

With respect to claims 3 and 13, the cited prior art fails to specifically teach an extended key preparing apparatus according to claim 2, wherein said nonlinear type operating unit performs nonlinear type operation in such a manner that when said cryptographic key is divided into eight elements of 32 bits by said dividing unit, said nonlinear type operating unit separates said elements into 6,5,5,5,5, and 6 bits to

transpose the same into other data, respectively, and the data after transposition are subjected to nonlinear type operation by the use of determinant.

The closest prior art, Ohmori (US pat 6,570,989), teaches a method of dividing a key into eight elements of 32 bits by a dividing unit, but then only separating the elements into four sets of 8 bits, not the set of 6,5,5,5,5, and 6 bits as stated in claims 3 and 13.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (571) 272-3874. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Andrew Caldwell
Andrew Caldwell

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

September 3, 2004